(1) Publication number:

0 308 219

ÇÎN 160 Pe 🔞 (1 MÎN) (BORRET MÎN, GERÎN (MEN A DE).

EUROPEAN PATENT APPLICATION

Manager A Tale 新新式機 Carlot Caracter A Carlot Carl Application number: 88308531.8 Secretary in the contract with the wind of a contract

The GRAND CONTRACTOR

(s) lint. Ct.4: G 06 F 12/14

2 Date of filing: 15.09.88

39 Priority: 18.09.87 US 98270

and the street of the street o

Drag growing and the second ार प्रातृत्यक्षा झारानुस्त्रका सक्तावस्त्र । हेन् द सम्बद्धारक्षात्र as uns de la como de Marie a made de 20

e to enterest a at gravitic equ

Marine Company of the

त्रा देशकार प्रदेशका के अधिकार है। इसका प्रकार के उन्हें इसकार प्रकार के अधिकार के अधिकार के अधिकार है। ्रम्भावत् । सम्बन्धाः, १८८ मा १ प्रस्तात् । १४ मा अभितासमूर्वानुष्ट्यः कृष्टिमान्नाः । १००० । १ ५ ००० १ सम्बन्धाः । Succeeded that considerance on the secondary of the second vinsans kapitan and song et fresh, mit jamit, i SECTION SECTION

> Date of publication of application: 22.03.89 Bulletin 89/12

(84) Designated Contracting States: AT BE CH DE ES FR GB GR IT LI LU NL SE

CESSEE 14、44、33、11、11、11、11000

Applicant: GENERAL INSTRUMENT CORPORATION 767 Fifth Avenue New York New York 10153 (US)

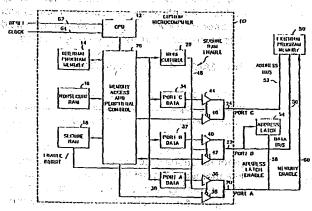
2 Inventor: Eyer, Mark K. 6737 Lipmann Street San Diego California 92122 (US)

> Moroney, Paul 1249 Avocet Court Cardiff-By-The-Sea California 92007 (US)

Representative: Blatchford, William Michael et al Withers & Rogers 4 Dyer's Buildings Holborn London EC1N 2JT (GB)

regrectively connected to ports A. B. and C. and a Microcomputer with internal RAM security during external program mode.

longo of Maricrocomputer which is operable in either an internal as an a ണ്ടാ ് mprogram mode; wherein the microcomputer functions in a ക്യൂഴ്ച accordance with an internally stored program, or in an external program mode, wherein the microcomputer functions in accordance with a program stored in a memory external to the microcomputer, provides internal RAM security during the external program mode. The microcomputer includes an internal program memory for internally storing programs; a bus for connection to an external memory for carrying programs from the external program memory; a nonsecure RAM for storing nonsecure data; a secure RAM for storing secure data; a central processing unit for processing the stored data and/or externally provided data either in accordance with the internally stored programs or in accordance with programs stored in the external memory; and a controller for controlling interconnections between the internal program memory, the bus, the RAMs and the central processing unit in accordance with the mode of operation of the microcomputer; wherein during the external program mode, the controller inhibits access to the secure RAM. Code for accessing the secure data stored in the secure RAM is contained in a program stored in the internal program memory. The microcomputer is ideally suited for performing cryptographic operations utilizing cryptographic keys stored in derived from the secure memory.



BEST AVAILABLE COPY

0

ш

Description

MICROCOMPUTER WITH INTERNAL RAM SECURITY DURING EXTERNAL PROGRAM MODE

10

15

25

30

35

55

BACKGROUND OF THE INVENTION

The present invention generally pertains to microcomputers and is particularly directed to providing security for data stored in the microcomputer when the microcomputer is operated in an external program mode.

A microcomputer essentially includes an internal program memory for internally storing programs; a bus for carrying data to and from the microcomputer; a random access memory (RAM) for storing data; a central processing unit for processing said stored data and/or data received over the bus in accordance with the internally stored programs; and a controller for controlling interconnections between the internal program memory, the bus, the RAM and the central processing unit in accordance with the mode of operation of the microcomputer.

For microcomputers that do not have an external program mode, wherein the operation of the microcomputer is in accordance with a program stored in an internal memory, the security of the data stored in the internal RAM is under the control of the program stored in the internal memory, and thereby security of such data may be assured. However, internal memory size is limited and may be enlarged only up to a certain point at which further expansion is not economically feasible because of increased silicon area and cost. Thus, for many applications, a microcomputer having an external program mode of operation is preferred for economic reasons:

In a prior art microcomputer having an external program mode of operation, the bus is connected to external memories for carrying programs from an external program memory and for carrying data from an external data memory; and the controller interconnects the bus to the internal RAM during the external program mode. Thus, operation of a prior art microcomputer in the external program mode affords an intruder access to the entire internal RAM, whereby sensitive data (such as access the internal RAM may be accessed from outside the accessed from outside the microcomputer and thereby compromised.

SUMMARY OF THE INVENTION

The present invention provides a microcomputer which is operable in either an internal program. mode, wherein the microcomputer functions in accordance with an internally stored program, or in an external program mode, wherein the microcomputer functions in accordance with a program stored in a memory external to the microcomputer, without compromising the security of data stored in a designated internal RAM. The microcomputer of the present invention includes an internal program memory for internally storing programs; a bus for connection to an external memory for carrying programs from the external memory; a nonsecure

RAM for storing nonsecure data; a secure RAM for storing secure data; a central processing unit for processing the stored data and/or externally provided data either in accordance with the internally stored programs or in accordance with programs stored in the external memory; and a controller for controlling interconnections between the internal program memory, the bus, the RAMs and the central processing unit in accordance with the mode of operation of the microcomputer, wherein during the external program mode, the controller inhibits access to the secure RAM. Code for accessing the secure data stored in the secure RAM is contained in a program stored in the internal program memory.

The microcomputer of the present invention is ideally suited for performing cryptographic operations. For cryptographic operations, the internal program memory stores a program for performing cryptographic operations upon data; and the secure RAM stores cryptographic key data required for performing the cryptographic operations.

Additional features of the present invention are described in relation to the description of the preferred embodiment.

BRIEF DESCRIPTION OF THE DRAWING

The figure of the drawing is a diagram of a preferred embodiment of the microcomputer of the present invention coupled to an external program memory.

DESCRIPTION OF THE PREFERRED **EMBODIMENT**

Referring to the Drawing, the preferred embodiment of the microcomputer 10 of the present invention includes a central processing unit (CPU) 12, an internal program memory 14, a nonsecure RAM-16, a secure RAM-18, buses 20, 22, and 24 respectively connected to ports A, B, and C, and a controller. The controller includes a memory-accodes, authenticators, or secure variables) stored in the 45% and entirely control unit 26, a mode control register 28, a port A data register 30, a port B data register 32, a port C data register 34, a first tri-state bus driver 36 coupling the port A data register 30 to the port A data bus 20, a second tri-state bus driver 38 coupling the memory-access-and-peripheralcontrol unit 26 to the port A data bus 20, a third tri-state bus driver 40 coupling the port B data register 32 to the port B data bus 22, a fourth tri-state bus driver 42 coupling the memory-accessand-peripheral-control unit 26 to the port B data bus 22, a fifth tri-state bus driver 44 coupling the port C data register 34 to the port C data bus 24, and a sixth tri-state bus driver 46 coupling the memory-accessand-peripheral-control unit 26 to the port C data bus 24. The fourth tri-state bus driver 42 is bidirectional. All of the other bus drivers are unidirectional and transfer data onto the respective port A, B and C buses 20, 22, 24 from the microcomputer 10.

10

15

30

35

40

45

50

55

65

The mode control register 28 provides a signal on line 48 indicating whether the microcomputer is in an internal program mode or an external program mode of operation. The mode indication signal on line 48 enables access to the secure RAM 18 during the internal program mode of operation and inhibits access to the secure RAM 18 during the external program mode of operation.

The port A bus 20 is a 2-bit control bus, which provides memory timing controls. The port B bus 22 is a multiplexed address/data bus, providing eight address bits and eight-bits of data for bidirectional transfer. The port C bus 24 provides eight additional

An external program memory 50 is coupled to the port A, B, and C buses 20, 22, and 24 of the microcomputer 10 by a 16-bit address bus 52, an address latch 54, an 8-bit data bus 56, an address latch enable line 58 and a memory enable line 60.

Additional input/output memory, or other peripheral devices may share the buses 20, 22, 24 along with the external program memory 50, given appropriate address decoding and interface circuitry. In the external program mode, the microcomputer 10 is, in effect, a general purpose microprocessor.

The CPU 12 receives reset and clock signals on

lines 62 and 64 respectively.

On reset, instructions are fetched from the internal program memory 14; and the mode control register 28 is set to indicate the internal program mode, and thereby provides a signal on line 48 that enables access to the secure RAM 18. Such an indication on line 48 also enables the bus drivers 36, 40 and 44 to respectively transfer the contents of the port A data register 30 onto the port A bus 20, the contents of the port B data 32 register onto the port B bus 22, and the contents of the port C data register 34 onto the port C bus 24. At the same time the internal program mode indication on line 48 inhibits the bus drivers 38, 42 and 46 from transferring data. When in the internal program mode, the CPU 12 has access to both the secure RAM 18 and the nonsecure RAM 16, as well as to all of the peripheral registers, including port A data register 30, port B data register 32, port C data register 34 and, mode control register 28.

When operating in the internal program mode, all instructions are executed from the internal program memory 14; and internal bus activity is not accessible at the pins of the microcomputer. In the internal program mode, access to external program

memory is not possible.

After power-up initialization is complete, program control may be passed to the external program memory 50 by first setting the mode control register. 28 to provide an external-program-mode indication signal on line 48 to inhibit access to the secure RAM 18, and then branching externally via bus drivers 38, 42 and 46. The external-program-mode indication signal on line 48 also inhibits the bus drivers 36, 40 and 44 from transferring data from the port A, B, and C data registers 30, 32 and 34 onto the port A, B, and C buses 20, 22 and 24. Program control may be returned to the internal program-memory 14-simply by branching to it.

When in the external program mode, the microcomputer's internal address and data buses are interconnected by the bus drivers 38, 42 and 46 to the external program memory 50, and control of the microcomputer is transferred to the external program memory 50. In the external program mode, access to the nonsecure RAM is allowed, while access to the secure RAM 18 is inhibited.

In a typical operating scenario, after system reset and initialization, control is passed to the external program memory 50. When data is available requiring authentication or comparison with variables stored in secure RAM 18, the data is written into the nonsecure RAM 16 and a branch is made to an entry point in the internal program memory 14. The mode control register 28 is then accessed to select the internal program mode, so that operations using secure data with nonsecure data may be performed. Internal secure routines are executed, with the results, if any, being written into the nonsecure RAM 16. Finally, the mode control register 28 is accessed to select the external program mode; and a return is made to the calling routine in the external program memory 50.

Whenever the program code provided from the external program memory 50 causes a switch to the internal program mode, any following instructions from the external program memory 50 are ignored. since the the switch to the internal program mode results in the mode control register 28 providing a mode indication signal on line 48 that inhibits the bus drivers 38, 42 and 46 from providing further access to the microcomputer by the external program memory 50. Since no device is available to place instruction data on the internal operating bus, the resulting value of zero is interpreted by the CPU 12 as a "do nothing" instruction. The microcomputer program counter then increments upwards until the first byte of the internal program memory 14 is reached, thus returning control to the internal program memory 50.

When the microcomputer 10 is adapted for performing cryptographic operations the programs stored in the internal program memory 14 contain cryptographic routines; and cryptographic keys and/or data required for deriving cryptographic keys are stored in the secure RAM 18. A "master" program stored in the external program memory 50 can utilize program subroutines stored in the internal program memory 14 to provide a "slave" cryptographic processor. This master program may be made to cause such a cryptographic processor to encrypt and store data, authenticate a block of data, and/or derive a new key from a previously stored key. Initially, data to be operated on by the cryptographic processor is placed in the nonsecure RAM 16 by the master program; and then the program branches to the internal program memory 16 for implementing the cryptographic processor. Cryptographic routines first enable the secure RAM 18; then access secure data, such as cryptographic keys, from the secure RAM 18; next perform cryptographic operations on the data; and finally store-any-results-of-such-cryptographic-processing in the nonsecure RAM 16. The microcomputer 10 is 4500

ijojika ini

15

20

1417

15 6

25

Marga.

then switched back to the external program mode to allow the results to be accessed from the nonsecure memory 16 and to allow further processing in the external program mode.

Preferably, the internal program memory 14 is a read-only memory (ROM). The secure RAM 18 of the microcomputer may be provided with nonvolatility (CMOS with battery backup, or EEPROM, for example). The secure RAM 18 of the microcomputer may then be loaded with secure data at one physical location and later shipped to another location where all but properly authorized transactions are pro-(i) hibited. A production of the Afficient transfer and the afficiency and a factors.

score with the common temporal tending to the line.

And sooms required as essented, smoot find

ingston in the control of the entropy of the conman Claims rago da a la la la hora rancama financia se obe a dalla with respondence of a may on porture of

A microcomputer that is operable in either an internal program mode, wherein the microcomputer functions in accordance with an internally stored program, or in an external program mode, wherein the microcomputer functions in accordance with a program stored in a memory external to the microcomputer, said microcomputer comprising

an internal program memory for internally dative: storing programs;

a bus for connection to an external memory for carrying programs from said external program arrana ramemory: 1000 atom the value are

a nonsecure RAM for storing nonsecure data; a secure RAM for storing secure data; ार होता हुन्य हुन्य क्षेत्र हेर्ने क्ष्म कर स्थापन होता है ज

The material is some to

with preference to 000 leader resources that the state performing cryptographs, specificate the programs stored in the internal program memory 14 pontain cryptographic routines; and cryptographic keys and/or data required for deriving cryptographic keys all stoned in the secure RAM 18, A "master" on yearn stored in the external program memory 66 edi di berris recinacidas marginal estilli. es foreign a although of all grounds margons in releting par cereng<mark>ong</mark> heresser, telt i spacecion interrigiority (i ineccuony didentificativa a ensistre de anenine. and the second received the sector are because the Malacesta a compagned was a reference forfair the

อีก เอเซอ อะครอด โดย เพลา เพลา เพลา เพลา เพลา

Will, Applied the optional Pauliness Control of the Pauliness Control of the Pauliness Control of the Contro

The court of the second control of the second of the secon

पुरा स्थान । प्राप्तु प्रतान हाम्युक्त अपूर्ण । एउट भी स्थितिस्था स्था । स्थान

, o no par va hatenina so ta caso in ocini casta in

advanced in the manufact Tax mideoceanable

and the amorate amorae and best privace income

and oyle of the mean of progent memory of the

Tourism at the memor property and the enemy

a central processing unit for processing said stored data and/or externally provided data either in accordance with said internally stored programs or in accordance with programs stored in said external memory; and

means for controlling interconnections between the internal program memory, the bus, the RAMs and the central processing unit in accordance with the mode of operation of the microcomputer;

wherein during said external program mode, the controlling means inhibits access to the secure RAM. Pobřeně 55 ali

2. A microcomputer according to Claim 1, wherein the controlling means comprise a mode control register for indicating the program mode; and Harry Carly Spile

a bus driver coupled to the mode control register for interconnecting the microcomputer with the bus to receive programs carried from the external memory over the bus during only the external program mode.

3. A microcomputer according to Claim 1, wherein the internal program memory stores a program for performing cryptographic operations upon data; and wherein the secure RAM stores secure cryptographic key data required for performing said cryptographic operations.

4. A microcomputer according to Claim 1, wherein the internal program memory stores a program containing code for accessing secure data from the secure RAM.

files and the capeciavely space of the second sectors

The grain after some or us some some strategisms to the shaper

unas to long with the effection of the the the

surrembered to the seed O magnetic that he warps

៖ ខ្ពស់ ១ - សេខស្លាសែ**ន ១០០៤ នាក**្សាស្ត្រ (៤០១៩) ៤ កំពីវ

40 (10) : - 1.50 (10) 28 (10 mosts 2. d) 168 (10 mill 1) 166 (1

Aprilia de la libraria de la seria de la composición del composición de la composición de la composición de la composición del composición de la composición

the converse of the second second and affection

RAM '8 and the nonsecure RAM 16, as well as to sal

of the peripheral registers, including port A date

register 30, cort 3 date register 32 port C datas

So jokom mujigara a nizati ati ni gadisaga monki.

revige of an earliest and permake one are an included

हरूको है। इस मेर क्यान वर्ष किन वर्षा व्यवस्थान है। हो हो**उंट**

in the second of the second of

inductification is noted toward in each property

province and a company of the province of the report from a security on all species and in 1991 to a 1994

And the Cape of the only all rates of the first to

ALCOHOL SEAL OF A BOOM ALCOHOLD DESCRICT

THE STREET OF STREET

one and in private and isometric time of the control

terfever 14 and, mode control register 26

salidio est son la exempara

n volular i kom er elemak (Strapsliger der i Auser

100 grant same in 150 grant messening on grant from 1.2.

55 Control of the contr

60े हो। एक एक आर्थ पर आरोपित वस्ता है अर्थ एक प्राप्त ta militar i killinden kallig indines i piloti i li se magnetic for the property of the control of the state of

